

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-39156

(43) 公開日 平成11年(1999) 2月12日

(51) Int. Cl.⁶
 G06F 9/06 550
 12/14 310
 320
 G09C 1/00 660

F I
 G06F 9/06 550 A
 550 Z
 12/14 310 Z
 320 B
 G09C 1/00 660 D

審査請求 未請求 請求項の数11 O L (全9頁)

(21) 出願番号 特願平9-195451

(22) 出願日 平成9年(1997) 7月22日

(71) 出願人 000005496

富士ゼロックス株式会社
 東京都港区赤坂二丁目17番22号

(72) 発明者 佐々木 茂彦
 神奈川県足柄上郡中井町境430 グリーン
 テクなかい 富士ゼロックス株式会社内

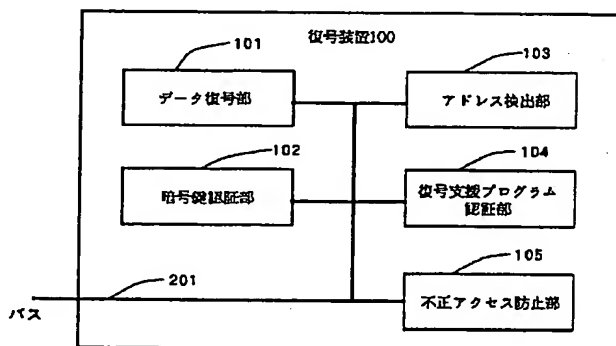
(74) 代理人 弁理士 澤田 俊夫

(54) 【発明の名称】 暗号化データ復号装置

(57) 【要約】

【課題】 復号支援プログラムの改竄により、暗号でプロテクトしたデータが不正に流用されることを防止する。

【解決手段】 復号指示を受けた復号装置100は、CPU202の動作を一時停止させる。アドレス検出部103は、CPU202のメモリアクセスを監視し、復号指示発行の命令コードの格納アドレスPrを取得する。暗号認証部102は、暗号鍵303の認証を行う。復号支援プログラム認証部104は、暗号鍵303から検証範囲指定(pre、post)を取得し、Pr-preからPr+postまでの領域について、一方向ハッシュ関数を用いたメッセージ要約数を算出し、この算出結果を、暗号鍵303中のメッセージ要約数502と比較し、復号支援プログラムの正当性を認証する。認証成功時、データ復号部101が、暗号鍵303から暗号の復号鍵501を取得し、暗号化データを復号する。



【特許請求の範囲】

【請求項1】 コンピュータ・システムに実装されて暗号化されたデータを復号する暗号化データ復号装置において、

暗号化されたデータを暗号鍵に基づき復号するデータ復号手段と、

上記暗号鍵が正当なものであることを認証する暗号鍵認証手段と、

CPUから復号指示の受取ったとき、復号支援プログラム中の上記復号指示を出した命令コードのメモリ・アドレスを検出するアドレス検出手段と、

上記命令コードのメモリ・アドレスに基づいて上記復号支援プログラムが正当なものであることを認証する復号支援プログラム認証手段とを有することを特徴とする暗号化データ復号装置。

【請求項2】 上記復号支援プログラムの実行中に割込み等で不正に処理の流れを奪われた場合に、それを検知し対抗処置をとる不正アクセス防止手段をさらに有する請求項1記載の暗号化データ復号装置。

【請求項3】 上記復号支援プログラム認証手段は、上記命令コードのメモリ・アドレスにより決定される所定のメモリ・アドレス範囲のコードの内容が真正なものであるかどうかを検証する請求項1または2記載の暗号化データ復号装置。

【請求項4】 上記所定のメモリ・アドレス範囲のコードの内容の所定の関数による計算結果に基づいて上記所定のメモリ・アドレス範囲のコードの内容が真正なものであることを検証する請求項3記載の暗号化データ復号装置。

【請求項5】 上記所定の関数を所定の一方方向性関数とする請求項4記載の暗号化データ復号装置。

【請求項6】 上記暗号鍵は、真正な復号支援プログラムから生成した参照値を保持し、上記復号支援プログラム検証手段による計算結果と、上記暗号鍵が保持する上記計算結果とを比較して上記復号支援プログラムの正当性が認証される請求項4または5記載の暗号化データ復号装置。

【請求項7】 上記暗号鍵は、上記所定のメモリ・アドレス範囲を指定する情報をさらに保持し、上記参照値は指定されたメモリ・アドレス範囲に基づいて生成される請求項6記載の暗号化データ復号装置。

【請求項8】 コンピュータ・システムに実装されて暗号化されたデータを復号する暗号化データ復号装置において、暗号化されたデータを暗号鍵に基づき復号するデータ復号手段と、

CPUから所定の情報がバスに転送されたとき、復号支援プログラム中にある、上記所定の情報を上記バスに転送した命令コードのメモリ・アドレスを検出するアドレス検出手段と、

上記命令コードのメモリ・アドレスにより決定される所定のメモリ・アドレス範囲の上記復号支援プログラムの内容に基づいて上記復号支援プログラムが正当なものであることを認証する復号支援プログラム認証手段とを有することを特徴とする暗号化データ復号装置。

【請求項9】 暗号化データを復号する暗号鍵本体と、上記暗号化データを復号するために用いる復号支援プログラムの所定の範囲のコードの所定の関数による計算結果と、上記暗号化鍵本体および上記計算結果に対する署名とを含む暗号鍵情報を生成する暗号鍵情報生成装置。

【請求項10】 暗号化データを復号する暗号鍵本体と、上記暗号化データを復号するために用いる復号支援プログラムの所定の範囲のコードの所定の関数による計算結果と、上記暗号化鍵本体および上記計算結果に対する署名とを含む暗号鍵情報を受け取るステップと、暗号化データを復号するときに、復号に用いる復号支援プログラムの上記所定の範囲に対応するメモリ領域に展開されたコードを取り出すステップと、上記取り出されたコードの上記所定の関数による計算結果を生成するステップと、

生成された上記計算結果と、上記暗号鍵情報中の上記計算結果とを比較するステップと、上記比較の結果に基づいて、上記復号に用いる復号支援プログラムの真正を検証するステップとを有することを特徴とする復号支援プログラム検証方法。

【請求項11】 バスと、上記バスに接続されたCPUと、上記バスに接続されたメモリと、上記バスに接続された認証装置とを有し、上記認証装置は、

上記CPUから暗号化データの復号指示が上記バスを介して転送されたとき、復号支援プログラム中にある、上記復号指示を出した命令コードのメモリ・アドレスを検出するアドレス検出手段と、

上記命令コードのメモリ・アドレスに基づいて上記復号支援プログラムが正当なものであることを認証する認証手段とを有することを特徴とするコンピュータ・システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、暗号化されたデータを復号する技術に関するものである。

【0002】

【従来の技術】従来、暗号方式をコンピュータ・システムに適用し、暗号化されたプログラムやデータを復号して利用する場合には、そのシステムの上で動作する復号プログラム（復号計算およびそれを支援するプログラム）を実行するのが一般的である（特開平3-68024号公報）。ところで、仕様が公開されたオープンなコンピュータ・システムにおいては、プログラムの解析お

よび改変が容易であるため、復号プログラムの復号支援部分（以下、復号支援プログラムともいう）を改変することにより、元の復号プログラムの仕様に反して、復号したデータを不正に利用することが簡単にできてしまい、システム全体の安全性は低くなるという問題があった。暗号方式の進歩はめざましく、強力な暗号強度をもつ暗号方式が多く提案されている。しかし、復号プログラムの解析、改変による問題は、使用している暗号方式の安全性には依存しないため、いくら高い強度をもつ暗号方式を採用しても、解決することはできない。

【0003】この問題を解決しようとする提案として、復号プログラム自体を暗号化し、データ復号時にのみ復号プログラムを復号して、データ復号作業を行う手段を採用し、これにより、復号プログラムの解析および改変を困難にするものが知られている（特開平 9 - 6 2 3 2 号公報）。しかし、復号プログラムを復号するのも、結局プログラムによって行われるため、本質的な解決になっておらず、解析と改変に要するコストを多少増加させるという効果しかない。しかも、近年のコンピュータの性能向上を考慮すると、増加するコストは大きな障害とはなり得ないため、復号プログラムの解析と改変を効果的に防止することができないという問題がある。また、いったん復号プログラムの改変に成功してしまえば、改竄プログラムの実行を防ぐことはできず、意図しない目的への復号したデータの流用の防止ができないという問題がある。

【0004】また、復号プログラムの改変を防止する手段として、CPU がメモリにアクセスするアドレスを監視して、予想される正当な復号プログラムのメモリアクセスパターンと比較した結果、正当と判断した場合は、メモリアクセスを許可するが、不正と判断した場合には、メモリアクセスを遮断することにより、意図しない不正なデータ利用を防止する提案がある（特開平 5 - 3 2 4 4 8 3 号公報）。しかし、機器組込用のプログラムが ROM で供給されるような特殊な小規模システムならば、プログラムは固定したアドレス位置に存在するため、CPU がアクセスするアドレスを監視することにより、復号プログラムの正当性の判断が可能だが、一般的なシステムでは、プログラムのロードされるアドレスは動的に決定されるため、アクセスするアドレス情報で復号プログラムを判定することができないという問題がある。また、不正判定基準のアクセスパターンを容易に変更することができないので、拡張性に乏しく、多くの暗号化データに対応することが難しい。そのため、この手法は一般的なコンピュータ・システムにおいて、使用することはできないという問題がある。

【0005】以上に述べたとおり従来の技術では、一般的なコンピュータ・システムにおいて、復号プログラムが改変されていない正当なものであることを、復号時に認証することができず、この結果、改変された復号プロ

グラムの実行を防ぐことができないかった。このため、改竄、改変された復号プログラムによる、復号したデータの意図しない目的への流用を効果的に防止できない。そのため、暗号方式の強度にかかわらず、システム全体の安全性は低くなってしまおうという問題がある。

【0006】

【発明が解決しようとする課題】本発明は、仕様が公開されたオープンなコンピュータ・システムにおいても、復号プログラムの正当性を暗号化データの復号時に認証できるようにし、これにより、改竄された復号プログラムによる意図しない目的への復号したデータの流用を防止することを課題としている。

【0007】

【課題を解決するための手段】本発明によれば、上述の目的を達成するために、コンピュータ・システムに実装されて暗号化されたデータを復号する暗号化データ復号装置に、暗号化されたデータを暗号鍵に基づき復号するデータ復号手段と、上記暗号鍵が正当なものであることを認証する暗号鍵認証手段と、CPU から復号指示の受取ったとき、復号支援プログラム中にある、上記復号指示を出した命令コードのメモリ・アドレスを検出するアドレス検出手段と、上記命令コードのメモリ・アドレスに基づいて上記復号支援プログラムが正当なものであることを認証する復号支援プログラム認証手段とを設けるようにしている。

【0008】この構成においては、復号支援プログラム中の復号指示を出した命令コードのメモリ・アドレスに基づいて、例えば、予め定められた領域のコードの内容を検証し、復号支援プログラムの正当性を認証できる。この場合、復号支援プログラムがメモリのどの領域にロードされていても検出した命令コードのアドレスを利用して適合理化できる。

【0009】

【発明の実施の態様】つぎに、本発明の実施例について、図面を参照して説明する。図 1 は、本発明の復号装置を用いて暗号化データを復号するコンピュータ・システムを示している。この実施例においては、コンピュータ・システムに実装された復号装置 100 と、コンピュータ・システムで実行される復号支援プログラムとにより暗号化データの復号を行う。

【0010】図 1 において、内部バス 201 に、CPU 202、I/O 部 203、復号装置 100、およびメモリ 205 を接続して、コンピュータ・システムが構成される。CPU 202 は、一般的なストアードプログラム方式のもので、メモリ 205 に格納されたプログラムコードを、内部バス 201 を介して読取って解釈を行い、読取ったプログラムコードの指示に従い動作する。システムの利用者は、CPU 202 に内部バス 201 を介して、I/O 部 203 とメモリ 205 に格納されたデータに、アクセスするよう、プログラムで指示を与えること

により、意図する通りにシステムを利用することができる。

【0011】図2は、図1の復号装置100の構成例を示す。この図において、復号装置100は、データ復号部101、暗号鍵認証部102、アドレス検出部103、復号支援プログラム認証部104、および不正アクセス防止部105を含んで構成されている。データ復号部101は、暗号化されたデータを暗号鍵に基づき復号するものである。暗号鍵認証部102は、その暗号鍵303（図5）が正当なものであることを認証するものである。アドレス検出部103は、CPU202から復号の指示の受取ったとき、復号支援プログラム301（図3）中にある、その復号指示を出した命令コードのメモリ・アドレスを検出するものである。復号支援プログラム認証部104は、復号支援プログラム301が正当なものであることを認証するものである。また、不正アクセス防止部105は、復号支援プログラム301の実行中に割込み等で不正に処理の流れを奪われた場合に、それを検知し対抗処置をとるものである。

【0012】図3は、暗号化されたデータを復号するときの、メモリ内のデータ格納状況を表したものである。図3において、復号支援プログラム301は、暗号化されたデータ302を復号して、復号データ格納領域304に格納するよう復号装置100に指令を出し、意図した目的のために復号データを利用するプログラムである。暗号鍵303（図5参照）は、暗号化データを復号するために必要な鍵データである。復号支援プログラム301、暗号化されたデータ302、暗号鍵303、復号データ格納領域304のメモリ205における格納アドレスは、p、c、kおよびdである。

【0013】図4は、復号支援プログラムのメモリ格納状態の概念図である。図4において、メモリ205上の、アドレスpからp...までが復号支援プログラム301が格納される領域である。復号支援プログラム301の中には、復号装置204に復号指示を発行する、復号指示発行部分402が含まれ、このコードが格納されるアドレスはprである。復号指示発行部分402のアドレスprから、前にpreバイト、後ろにpostバイトで区切ったブロックが、復号支援プログラム検証ブロック403である。復号支援プログラム検証ブロック403のメッセージ要約数を用いて、復号支援プログラムの正当性を判断する。preとpostは、暗号鍵303で指定される（図5参照）。

【0014】図5は、暗号鍵303の構成図である。暗号鍵303はデジタルデータであり、暗号の復号鍵501、復号支援プログラムのメッセージ要約数502、検証領域範囲指定503、および暗号鍵全体の署名504から構成される。

【0015】図6は、暗号鍵303を生成する暗号鍵生成装置の構成例を示しており、図6において、暗号鍵生

成装置は検証範囲指定部505、復号支援プログラム入力部506、復号鍵入力部507、メッセージ要約数生成部508、署名生成部509および暗号鍵出力部510を含んで構成されている。検証範囲指定部505は、復号指示コードのアドレス、検証ブロックを特定するバイト数preおよびpostを受け取る。メッセージ要約数生成部508は、検証範囲指定部505で指定された範囲で復号支援プログラムのメッセージ要約数を生成する。署名生成部509は、復号鍵入力部507から入力された復号鍵、検証ブロック指定情報のバイト数preおよびpostおよびメッセージ要約数生成部508で生成したメッセージ要約数に対して署名を生成する。暗号鍵出力部510は、復号鍵、メッセージ要約数、ブロック指定情報のpreおよびpost、署名を一体にして出力する。

【0016】つぎに、本実施例の復号処理について説明する。本実施例では、復号処理は復号支援プログラム301および復号装置100が共同して行う。図7は、復号支援プログラム301のフローチャートである。図8は、復号装置100の処理の流れを表すフローチャートである。図7において、暗号化データを復号するために、復号支援プログラム301の実行が開始されると、まず前処理が行われる（ステップ601）。前処理では、暗号化データ302と暗号鍵303をメモリ205にロードし、復号データを格納する領域304を確保して、図3に示す通りにメモリ格納状況を構成する作業や、その他の必要な前処理作業を行う。次に、暗号鍵の格納アドレスk、暗号化データの格納アドレスc、復号データの指定格納アドレスdを復号装置100に与える。具体的には内部バス201を通じて、復号装置100にマップされたI/Oアドレスに、k、c、dを出力することにより行う（ステップ602）。もちろん、別の方法で復号装置100と通信しても構わない。

【0017】この後、復号装置100に復号処理を行うよう指示を発行する（ステップ603）。このとき、ステップ603に相当する命令コードが格納されているアドレスがPrである。この指示の発行は、具体的には、内部バス201を通じて、復号装置100にマップされたI/Oアドレスに、指示命令を出力することにより行われる。

【0018】復号を行う復号装置100は、内部バス201を介して、CPU202がどのようなアクセスをしているかを、監視することができる。また、CPUを介さずに直接メモリにアクセス（DMA: Direct Memory Access）することができる。加えて、CPU202の動作を制御し、必要に応じてCPU202を一時停止状態に保ったり、動作を再開させることができる。

【0019】図8において、復号指示を受けた復号装置100は、ステップ701において、ただちにCPU2

02の動作を一時停止させ、暗号鍵303の格納アドレスk、暗号化データ302の格納アドレスc、復号データの指定格納アドレスdを読取る(ステップ701)。これにより復号支援プログラム301はステップ603で一時停止状態となる。以下の復号装置100のメモリ205へのアクセスはすべてDMAを用いる。

【0020】復号装置100の処理はステップ702に進む。ステップ702では、CPU202のメモリ205へのアクセスの監視によって、復号指示発行の命令コードの格納アドレスPrを取得する。

【0021】次にステップ703において、暗号鍵303の認証を行う。暗号鍵303には、暗号鍵全体の署名504が用意されており、電子署名認証技術により、正当な暗号鍵であるか認証する。具体的には、復号装置には署名認証鍵が用意されており、RSA(Rivest-Shamir-Adelman)公開鍵暗号技術と、一方向ハッシュ関数を用いたメッセージ要約生成技術を用いて認証を行う。もちろん、他の方式で認証しても構わない。

【0022】もし認証に失敗した場合は、暗号鍵303が改竄されている可能性がある。復号装置100は、暗号鍵303が正当なものでないを見なし、ステップ705に進む。ステップ705において、CPU動作を再開させ、CPUに「暗号鍵の認証に失敗」を意味するエラーコードを返す。具体的には、復号装置100にマップされたI/Oアドレスにアクセスすることにより、CPU202が読出すことができるレジスタにエラーコードを格納する。もちろん、別の方法でCPU202と通信しても構わない。動作を再開した復号支援プログラム301では、ステップ605の分岐でエラーが発生したと判断し、ステップ606でエラー処理を行い、復号を行わずに終了する。

【0023】ステップ703において暗号鍵303の認証に成功した場合は、ステップ704へ処理を進める。ステップ704において、暗号鍵303から検証範囲指定503を取得し、Pr-preからPr+postまでの領域について、一方向ハッシュ関数を用いたメッセージ要約数を算出する。

【0024】続いて、ステップ706において、暗号鍵303中の復号支援プログラムの検証領域のメッセージ要約数502と、前ステップ704で算出したメッセージ要約数を比較する。もしこれらが一致しなかった場合、CPU202が実行している復号支援プログラム301が、暗号鍵303の発行者が意図したものと異なることを意味する。復号装置100は、復号支援プログラム301が改竄されたものと見なして、ステップ707に進む。ステップ707において、CPU202の動作を再開させ、CPUに「復号支援プログラムの認証に失敗」を意味するエラーコードを返す。具体的には、復号装置100にマップされたI/Oアドレスにアクセスす

ることにより、CPU202が読出すことができるレジスタにエラーコードを格納する。もちろん、別の方法でCPU202と通信しても構わない。動作を再開した復号支援プログラム301は、図7のステップ605の分岐でエラーが発生したと判断し、ステップ606でエラー処理を行い、復号を行わずに終了する。

【0025】図8のステップ706で復号支援プログラムの認証に成功した場合は、ステップ708へ処理を進める。ステップ708において、復号装置100は、暗号鍵303から暗号の復号鍵501を取得して、暗号化されたデータの復号処理を行う。具体的には、暗号の復号鍵と復号装置の装置ごとに別々のものが用意されている秘密鍵の2つから、DES(Data Encryption Standard)等のブロック暗号の復号鍵を生成し、ブロック暗号復号器に、DMAで暗号化されたデータを読出し、復号結果をDMAで復号データ領域に書出す。もちろん、どのような方法の暗号/復号方式を用いても構わない。

【0026】復号処理が終わった後は、ステップ709に進み、復号したデータを利用する。利用後は必要に応じて、復号したデータをメモリ205から消去することにより、意図しない目的に復号したデータを用いられることを防止できる。

【0027】また、復号装置100は、CPU202の内部バス201へのアクセスを監視することにより、復号支援プログラム301がCPU202により実行されている間に不正な割込み等により処理の流れを奪う操作を検知できる。不正に処理の流れが奪われたことを検知した場合、復号作業を即刻中止し、それまでに復号したデータもDMAにより破壊する。この機能により、ハードウェア割込みによるプログラムの動作への干渉を排除することができ、さらに安全性が向上する。

【0028】

【発明の効果】以上説明したように本発明は、復号支援プログラムの正当性を、復号時にチェックすることにより、改竄された復号支援プログラムによる意図しない目的への復号したデータの流用を防止する。これにより、復号支援プログラムの耐改変性を高めることができ、暗号強度に見合ったシステムの安全性を得ることができ

【図面の簡単な説明】

【図1】 本発明の実施例のコンピュータ・システムの構成を示すブロック図である。

【図2】 上述実施例の復号装置の構成を示すブロック図である。

【図3】 暗号化されたデータを復号するときのメモリ内のデータ格納状況を説明する図である。

【図4】 復号支援プログラムのメモリ格納状態の概念的に示す図である。

【図5】 暗号鍵の構成を説明する図である。

【図 6】 暗号鍵を生成する暗号鍵生成装置の構成例を示すブロック図である。

【図 7】 復号支援プログラムの動作を説明するフローチャートである。

【図 8】 復号装置の処理の流れを説明するフローチャートである。

【符号の説明】

100 復号装置

101 データ復号部

102 アドレス検出部

103 復号支援プログラム認証部

104 不正アクセス防止部

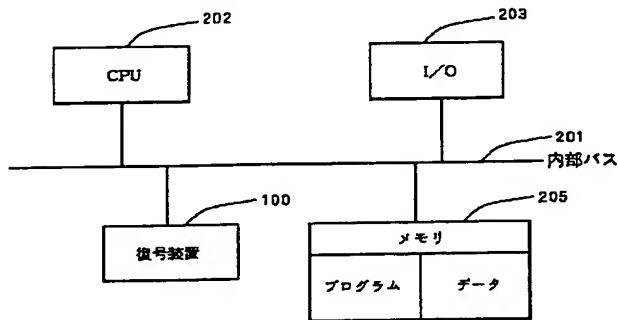
201 バス

202 CPU

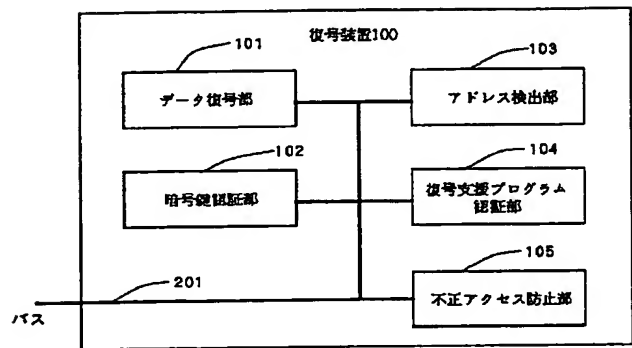
203 I/O部

205 メモリ

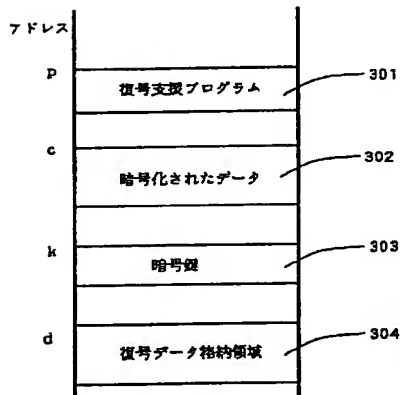
【図 1】



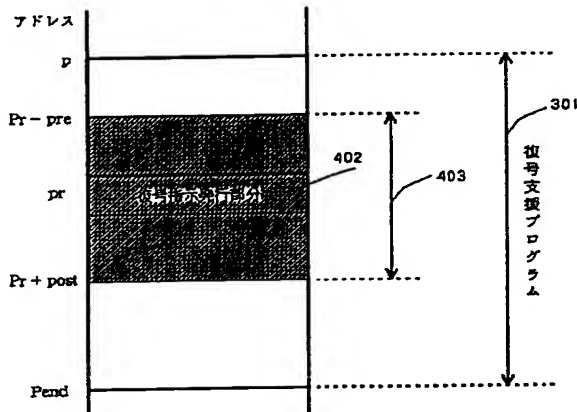
【図 2】



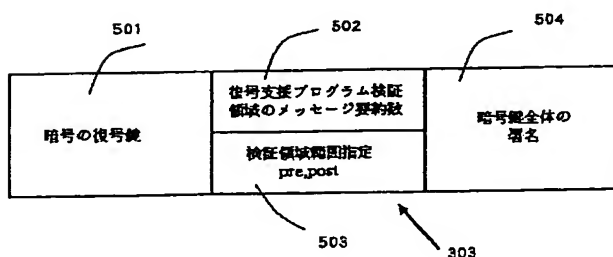
【図 3】



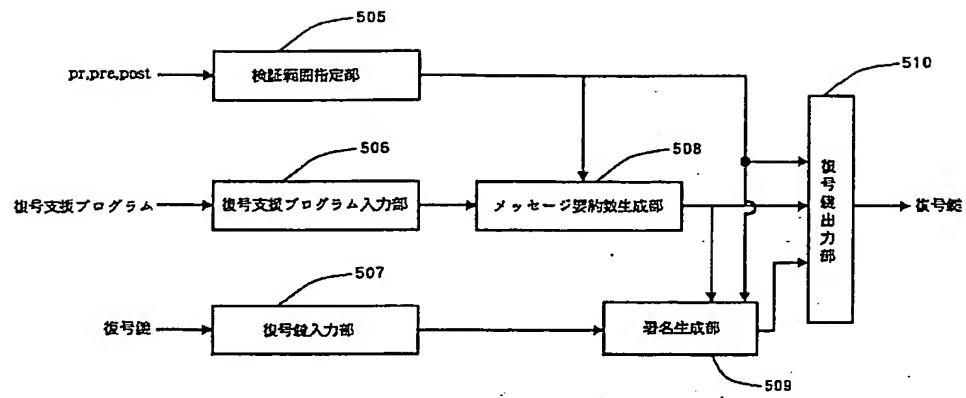
【図 4】



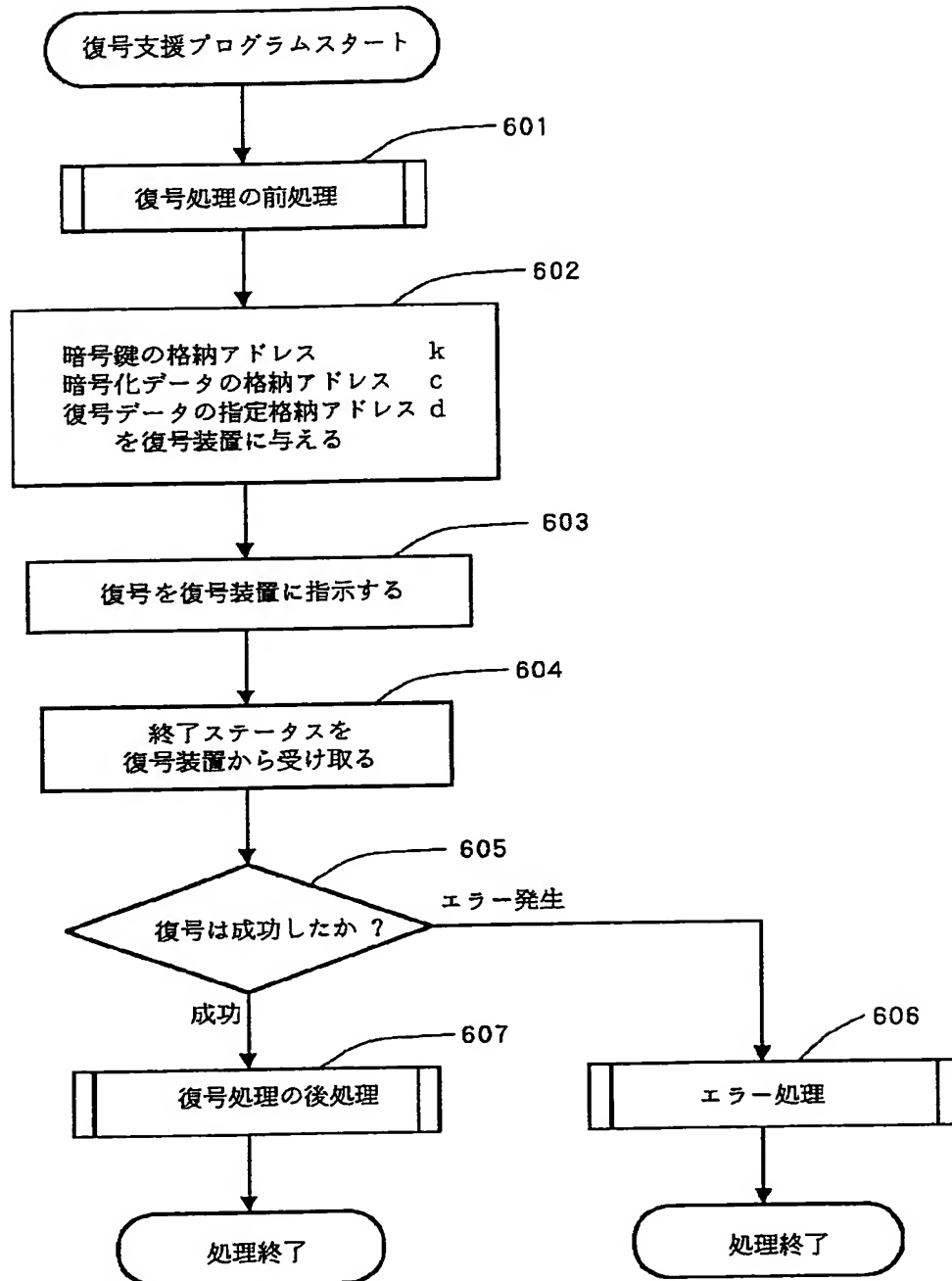
【図 5】



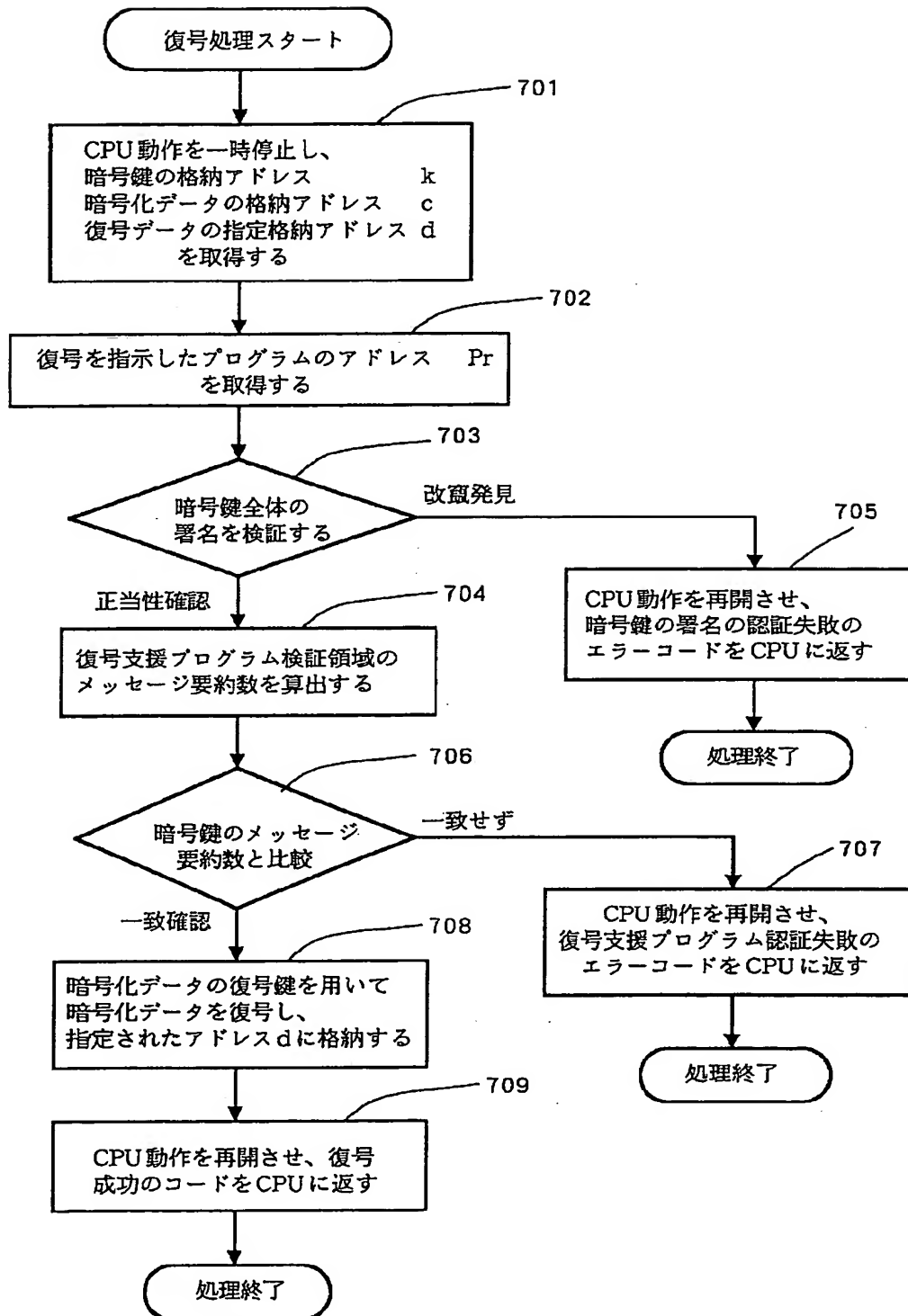
【図 6】



【図 7】



【図 8】



THIS PAGE BLANK (USPTO)